



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Secure Web Fingerprint Transmission (SWFT)
--

Defense Manpower Data Center (DMDC)

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

- ☐ (1) Yes, from members of the general public.
- ☒ (2) Yes, from Federal personnel* and/or Federal contractors.
- ☐ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.
- ☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

- ☐ New DoD Information System ☐ New Electronic Collection
- ☒ Existing DoD Information System ☐ Existing Electronic Collection
- ☐ Significantly Modified DoD Information System

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

- ☐ Yes, DITPR Enter DITPR System Identification Number
- ☐ Yes, SIPRNET Enter SIPRNET Identification Number
- ☒ No

c. Does this DoD information system have an IT Investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

- ☐ Yes ☒ No

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

- ☒ Yes ☐ No

If "Yes," enter Privacy Act SORN Identifier

DMDC nn DoD (Not Assigned)

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: <http://www.defenselink.mil/privacy/notices/>

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an OMB Control Number?

Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☒ **Yes**

Enter OMB Control Number

In Process

Enter Expiration Date

☐ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

DoD Directive 5200.5, DoD Personnel Security Program (32 CFR part 156); DoD Directive 5105.42, Defense Security Service; E.O. 9397 (SSN)

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

- (1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

To provide means for the National Industrial Security Program (NISP) contractors to submit electronic fingerprints and personal information to the Defense Manpower Data Center (DMDC) for applicants who require a background investigation by the Office of Personnel and Management (OPM) for a personnel security clearance. Cleared contractors collect and securely transmit electronic fingerprints to SWFT for transmittal to OPM.

Types of personal information collected in SWFT include: Social Security Number, Name, place of birth, date of birth, Electronic fingerprint file.

- (2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

The privacy risks associated with PII collection and the SWFT application are low. Defense-in-depth security measures are in place to protect PII data. Users/operators must be identified, authenticated, and authorized through multiple physical and logical security layers before any data may be accessed. Additionally, to guard against unwanted information disclosure and to protect the data from unauthorized modification, while in transit, all electronic communication is transmitted via secure channels using, at minimum, SSL 3.0/TLS 1.0. Furthermore all data at rest is encrypted using a FIPS 140-2 validated cryptographic module. These security measures meet or exceed the minimum required by DoD directives and the Security Technical Implementation Guides (STIGs). Finally, the system is subject to routine internal security reviews, as well as, a yearly outside audit.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

- ☐ **Within the DoD Component.**

Specify.

- ☐ **Other DoD Components.**

Specify.

- ☒ **Other Federal Agencies.**

Specify.

- ☐ **State and Local Agencies.**

Specify.

- ☐ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify.

- ☐ **Other** (e.g., commercial providers, colleges).

Specify.

i. Do individuals have the opportunity to object to the collection of their PII?

☒ **Yes**

☐ **No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

Information provided by individuals for a security clearance is voluntary. Without voluntary disclosure of information on a DLAH Form 1728 an investigation cannot be completed in a timely manner and may negatively affect an individual's placement or security clearance prospects. If an individual objects to sharing the required personal information needed to initiate a security clearance then the individuals clearance request cannot be processed.

(2) If "No," state the reason why individuals cannot object.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

☒ **Yes**

☐ **No**

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

The DLAH Form 1728 is used to initiate or reinvestigate a person's eligibility for security clearance access. The DLAH Form 1728 provides a list of Privacy Act Routine Uses under which a subjects information may be accessed by other than the person who is the subject of the DLAH Form 1728. When a subject signs and submits their DLAH Form 1728 they consent to those Privacy Act Routine Uses.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒ Privacy Act Statement

☐ Privacy Advisory

☐ Other

☐ None

Describe each applicable format.

DLAH Form 1728 – Privacy Act Statement

AUTHORITY: 10 U.S.C. 133, Under Secretary of Defense for Acquisition and Technology; E.O. 9397 (SSN); E.O. 10450 (Security Requirements for Government Employees); and DLA Privacy Act System Notice S500.50, available at <http://www.defenselink.mil/privacy/notices/dla/>.

PRINCIPAL PURPOSE(S): Information is collected to allow us to issue you a building badge. The badge is used to control access to and movement on DLA installations, buildings, or facilities.

ROUTINE USES: Information you provide may be disclosed for any of the Routine Uses published by DoD at <http://www.defenselink.mil/privacy/notices/blanket-uses.html> Contact the system manager or your local Privacy Act Officer for further details.

DISCLOSURE: Disclosure is voluntary. However, failure to provide the requested information will result in our inability to issue you a badge or grant you access to DLA installations, buildings, or facilities.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.